Universidade Federal de Uberlândia - UFU
Prof. Rodrigo Sanches Miani

Atividade 3 – Criptografia simétrica

Objetivo: Familiarizar os alunos com os conceitos de criptografia simétrica.

Ferramentas: ghex e openssl.

Tarefas

1. Cifragem e decifragem usando diferentes algoritmos.

   (a) Crie um arquivo texto com o seu nome completo e número de matrícula.

   (b) Crie três chaves K1, K2 e K3 em hexadecimal. A chave K1 deve ter 56 bits, a chave K2 deve ter 128 bits e a chave K3 deve ter 256 bits.

   (c) Crie um vetor de inicialização IV em hexadecimal com 56 bits. Esse vetor de inicialização é parte integrante dos algoritmos simétricos pois é à partir dele que são adicionadas questões de aleatoriedade no processo de cifragem. Na prática, esses vetores são criados à partir de números aleatórios e transmitidos em claro juntamente com a mensagem.

   (d) Use o openssl para cifrar o arquivo texto criado anteriormente usando os algoritmos DES (cbc) e AES (128 bits e 256 bits - cbc). O link mostra o uso da função "encryption" e “decryption” do openssl - https://www.openssl.org/docs/manmaster/man1/openssl-enc.html. Não se esqueça de criar arquivos de saída diferentes para cada algoritmo de criptografia. Você deverá ter ao todo três arquivos cifrados.

   (e) Decifre os três arquivos e mostre que eles são iguais aos originais.

2. Tente visualizar os arquivos cifrados. Mostre os resultados. É possível visualizar os arquivos cifrados?

3. O arquivo pic_original.bmp presente no Moodle contém uma simples figura. Gostaríamos de cifrar essa figura para que as pessoas não saibam o conteúdo da mesma.

   (a) Cifre a figura usando o algoritmo AES no modo ECB e no modo CBC. Use as chaves criadas no Exercício 1.

   (b) Tente visualizar os arquivos cifrados usando um visualizador de imagens qualquer. Descreva os resultados.

(c) Edite o arquivo original usando um editor de arquivos hexadecimal (ghex, por exemplo) e copie os primeiros 54 bytes do arquivo. Observação: em um arquivo .bmp, os 54 bytes funcionam como um cabeçalho de informações para a figura.

(d) Edite os arquivos cifrados usando o editor de arquivos hexadecimal e sobrescreva os 54 primeiros bytes de cada um deles pelos bytes do arquivo original. Visualize cada um dos arquivos cifrados. O que aconteceu? Explique os resultados.

(e) Escolha uma outra figura qualquer e repita o procedimento acima. Relate as suas observações sobre esse novo experimento.